UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with email addresses cosma2k@gmail.com, and demsoft@gmail.com that are stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA.

Case No. 15-888 M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

The application is based on these facts: See attached affidavit.

☒ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached affidavit.

Applicant's signature

Lee Chartier, Special Agent, Federal Bureau of Investigation

Printed Name and Title

Sworn to before me and signed in my presence:

Date: June 5, 2015 at 9:35 AM

Judge's signature

City and State: Milwaukee, Wisconsin

William E. Callahan, Jr., U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Lee R. Chartier, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain account that are stored at premises controlled by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since November 2007. I am currently assigned to the FBI Milwaukee Division's Computer Intrusion Task Force. Prior to becoming a Federal Agent, I worked in a variety of public and private positions in the Information Technology industry.

3. As a Special Agent with the FBI, I investigate criminal and national security-related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of spam, malicious software, the theft of personally identifiable information, and other computer related fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received education

and training in computer technology, and computer-based fraud, and I have held industry certification from Microsoft and CompTIA.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(2), (a)(5)(A), (c)(2)(A), (c)(4)(B), and (c)(4)(G) have been committed by Dmitry Nizhegorodtsev. There is also probable cause to search the information associated with email addresses **cosma2k@gmail.com** and **demsoft@gmail.com** (as further described in Attachment A) for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. A confidential source of information working for the Federal Bureau of Investigation (CS-1) provided significant information regarding Dmitry A. Nijegorodtsev. CS-1 has been cooperating with U.S. law enforcement since approximately August 2012. CS-1 has a prior conviction for computer related crimes. CS-1 is cooperating in exchange for a reduced sentence and monetary support. CS-1 has provided law enforcement with timely and reliable information that has been corroborated through subsequent recorded conversation and controlled

buys. This information has resulted in the issuance of criminal complaints against three individuals.

8. In interviews, CS-1 identified "Cosma" as the operator of the Rustock botnet, whose true name is Dmitry A. Nijegorodtsev (also translated as Dmitry Novogorodtsev). CS-1 stated that Nijegorodtsev also uses the aliases or online monikers Cosma2k, Dem, Demetrius, and William Hanna. CS-1 produced pictures of Nijegorodtsev. Based on previous dealings with Nijegorodtsev while CS-1 was engaged in spamming activities, CS-1 knew Nijegorodtsev to be approximately 33 years old and living in Moscow, Russia. CS-1 knows Nijegorodtsev to be involved in botnets, spamming, fake anti-virus, and penny stock fraud, and that Nijegorodtsev was able code / program malicious software to perform the various computer crimes. CS-1 identified email and ICQ accounts Nijegorodtsev had used in the past, including: **demsoft@gmail.com**, **cosma2k@gmail.com**, mail@dempost.ru, demetrius@bk.ru, and ICQ# 73222222.

Affking Affiliate Network

9. On August 9, 2009, in federal district court for the Eastern District of Missouri, defendant Jody M. Smith pled guilty to a one-count information charging a conspiracy to traffic in counterfeit Rolex watches. The investigation into Smith revealed, and Smith admitted in his guilty plea, that he contracted with "spammers" or senders of spam emails to solicit customers to purchase his counterfeit Rolexes. Smith admitted that he paid more than $2,000,000 to the spammers to send the email messages.

10. As part of the investigation into Smith's case, the FBI, assisted by the Federal Trade Commission (FTC), determined that Smith's enterprise, which operated both within and

outside the United States, was named "Affking." The FTC received over three million complaints regarding spam messages connected to this operation.

11. In his guilty plea, Smith identified Australian citizen and resident Lance Atkinson as a co-conspirator in the Affking email marketing and counterfeiting operation. Based on other undercover investigation, the FBI and FTC determined that in addition to selling counterfeit Rolexes, Affking also deceptively marketed and sold counterfeit herbal "male enhancement" pills and generic prescription drugs that were falsely advertised as FDA-approved.

12. As part of the ongoing investigation into Smith, Atkinson, and Affking, the United States government sought assistance from Australian and New Zealand authorities. On December 23, 2008, Lance Atkinson was interviewed by the Australian Communications and Media Authority. The purpose of the interview was to get the details of Atkinson's and Smith's spam enterprise.

13. In the interview, Atkinson explained his involvement in the Affking and related enterprises, included Affking predecessor companies Genbucks and Sancash. Atkinson admitted that, using a nickname, he posted message on a pro-spam Internet bulletin boards seeking spammers to promote the herbal pills. In particular, Atkinson recalled that his largest spamming affiliates were Russian. Specifically, he recalled that two of his largest Russian spamming affiliates used the online monikers "Docent" and "Dem." Atkinson also admitted that he also used banner advertisements on websites and advertisements placed within Internet search engines to market to products. Atkinson estimated that 80% of all the advertising was done by the affiliates via spam emails, with the other 20% done through banner and internet search engine advertisements.

14. I am aware that after Atkinson was interviewed, he returned to illegal sales of herbal supplements and continued this operation at least until Nizhegorodtsev botnet, nicknamed the "Rustock botnet" was disabled by Microsoft in September 2011, as described below.

15. On June 15, 2012, in federal district court for the Eastern District of Wisconsin, defendant Oleg Y. Nikolaenko pled guilty to a two-count superseding indictment charging that he knowingly caused the transmission of a program, information, code, and command that caused, and attempted to cause, the transmission of multiple commercial electronic mail messages between January 2007 and November 2010. As a result of such conduct, Nikolaenko intentionally caused damage without authorization to a protected computer and caused at least $5,000 in loss to one or more persons during a one-year period.

16. As part of his guilty plea, Nikolaenko admitted that he was a spammer who used the online moniker "Docent." He also admitted that he worked with Lance Atkinson, his brother Shane Atkinson, and other spammers to send spam emails to promoting Genbucks' products.

17. The forensic analysis of the computer also revealed that Nikolaenko had several chats with ICQ# 73222222, who was using the alias "William Hanna." In the logs, Hanna and Nikolaenko discussed the damage that was done to Nikolaenko's botnet when U.S. security company FireEye temporarily disabled Nikolaenko's botnet:

> (6:13:53 PM) Nikolaenko: ну не все порегали конечно и можно вернуь. но там не многа [not all, still can get it back, but not too many bots lost]
>
> (6:14:11 PM) Nikolaenko: с таким качеством трафа, как было в последнее время. там наверное вообще все сдохло) [with that kind of traffic they all dead probably]
>
> (6:14:19 PM) william hanna: ну файрай как всегда немного преувеличил что там окло 700к было ботов =) [fireeye like always exaggerated about 700k]

(6:14:40 PM) william hanna: или маршал.. не помню точно но читал что там 700к ботов было =) [or marshall. I dont remember but for sure i've read about 700k bots]

(6:29:07 PM) william hanna: т.к. я слал спампромо с 3к ботов всего =) [because I spammed spampromo (another pharmacy affiliate program) from only 3k bots

(6:29:16 PM) william hanna: у меня за день было около 6к уников трафа и 5 сейлов [in one day I had around 6k uniq clicks\traffic and 5 sales]

(6:29:28 PM) william hanna: а тут шлет в 20 раз больше и трафа всего в 3 раза больше =) [and here I have 20 times more bots spamming(sending emails) and only 3 times more traffic]

(6:30:20 PM) Nikolaenko: на твоем месте) пока спамит работает) [on your place. As long as spamit works]

(6:30:51 PM) william hanna: да я и не связываюсь =) у меня ботнет простаивает с 3к шлющими онлайна =) вот и поставил пробануть =) 530 баков заработал =) [im not dealing with him. I have inactive botnet with 3k mailing bots online. So I tried it. Made 530 $]

iContact Data Breach and Spam

18. The following day, "William Hanna" again chatted with Nikolaenko. In that chat, Hanna, admitted, "I have stolen database from iContact+", and "156k records with addresses etc."

19. The text of the December 10, 2009, chat between Nikolaenko and "Hanna" (ICQ# 73222222) is translated as follows:

(11:08:28 PM) william hanna: у меня база есть спизженная с iContact +ConstantContact [I have a database that was stolen from iContact + ConstantContact]

(11:08:33 PM) william hanna: чисто стокеры =) [only stockers (brokers?]

(11:08:39 PM) william hanna: 156к записей с адресами и т.д. [156k records with addresses, etc]

(11:08:55 PM) Nikolaenko: только их н7е ботами надо [You should use h7e bots]

(11:09:12 PM) william hanna: ботами можно только определенным методом =) [You have to use bots in a certain way]

20. Based on interviews with the company and online information, I am aware that iContact is an email marketing service that allows businesses, non-profit organizations, and associates to create, send, and track email newsletters, surveys, and auto responders. Their service is used by over 460,000 users. As of 2009, their database contained slightly over one billion email addresses. On or about February 8, 2010, iContact, which is headquartered in Raleigh, North Carolina, contacted the FBI and stated that it began receiving complaints from their client's customers regarding the receipt of unsolicited emails in December of 2009.

21. According to security personnel from iContact, iContact's customers believed iContact was responsible for the spam because the recipients of the spam had only provided their respective email addresses to be included in iContact mailings, but the spam emails were received shortly after signing up for their service. iContact employees also noticed an increase in unsolicited email to their corporate accounts around the same time of these complaints. iContact reviewed the spam emails and confirmed that the alleged senders of spam all had "@icontact.com" email addresses, confirming that the contents from their email database had been used for spamming purposes by an unknown third party.

22. More than 105 companies located in the State and Eastern District of Wisconsin were customers of iContact in December 2009. iContact estimated the theft encompassed their entire customer database. iContact estimated the potential loss related to the loss of all email addresses maintained by iContact and all system remediation activities related to these intrusions is approximately $20,000,000. This figure does not include any possible secondary victimization based on any loss of client credit card and other personal identifiable information.

Microsoft Civil Action Against Rustock Botnet

23. In September 2011, Microsoft Corporation obtained civil injunctions in U.S. District Court for the Western District of Washington (Case (No. 2:11-cv-00222), requiring that all U.S. internet service providers named therein take certain named and known servers, domain names, and IP addresses offline. Microsoft established that the targeted servers, domain names, servers and IP addresses were being used to host a botnet nicknamed "Rustock." According to one spam expert, Paul Wood, MessageLabs Senior Intelligence Analyst for Symantec Hosted Services, prior to September 2011, Rustock was the single largest botnet in the world, believed to have control of 1.1 million to 1.7 million compromised computers globally. This expert opined that at the end of 2010, Rustock was responsible for as much as 47.5 percent of all global spam. In March of 2011, expert Paul Wood believed Rustock was capable of sending almost 30 billion emails per day and was one of the world's largest spam botnets.

24. Microsoft's civil action against the Rustock botnet identified computers that were being used by the operator of the Rustock botnet as command and control for the botnet. According to Microsoft's court filings, the operator of Rustock told an individual who buys and resells access to computers for storing files that he resided in St. Petersburg and is known to the reseller and in online forums under the nickname "Cosma2k."

25. The hosting reseller had communicated with "Cosma2k" at three ICQ numbers, including 73222222. Microsoft employees also averred that its research regarding the nickname "Cosma2k" indicates that it (1) is associated with the names "Dmitry Novgorodtsev," "Dmitry Nijegorodtsev," and nicknames "Demetrius," "Demetrius Software," and (2) is associated with the email address **cosma2k@gmail.com**, mail@dempost.ru , admin@netbiz.ru., and two others.

Further Identification of Email Addresses

26. Based on the identifiers provided by CS-1 and Microsoft, as well as the information gleaned from the prosecutions of Jody Smith and Oleg Nikolaenko, further research was done to identify Dmitry Novgorodtsev and any email addresses he may use.

27. A posting on Google Groups (groups.google.com/forum/#!topic/news.admin.net-abuse.blocklisting/qAkRwbk6wOs) revealed that email address **cosma2k@gmail.com** was used to register the domain "demsoft.net." The name associated with that registration was "Dmitry Nijegorodtsev."

28. Online, publically available searches for email addresses associated with Novgorodtsev by CS-1 and Microsoft reflected that the email **demsoft@gmail.com** was used to register an account on the website http://aeroboard.ru/member7453.html under the name Demetrius.

29. On September 11, 2014, a subpoena was issued to Google for information related to the email addresses **demsoft@gmail.com**, and **cosma2k@gmail.com**. Google's response to the subpoena revealed that email address **demsoft@gmail.com** was registered on February 3, 2005 under the name: Stepan Saveliev with the recovery email: mail@dempost.ru. The subpoena showed a login and logout action on the **demsoft@gmail.com** account in March 2014 and June 2014. Both of the IP addresses used to access the account were from Tor servers (Tor is a free software for enabling online anonymity and is designed to make it possible for users to surf the internet anonymously). Based on my training and experience, I am aware that Tor servers are regularly used by criminals on the internet so their activities and location cannot be discovered.

30. Google's response to the subpoena revealed that email address **cosma2k@gmail.com** was registered on April 27, 2005 under the name: Cosma Cosmosis with the recovery email: support@defile.ru. The subpoena showed the **cosma2k@gmail.com** account was accessed 9 times from March 2014 to June 2014. Several of the IP addresses used to access the account were from Tor servers. Based on my training and experience, I am aware that Tor servers are regularly used by criminals on the internet so their activities and location cannot be discovered.

31. I have caused previous preservation requests to be sent to Google regarding these gmail addresses. I am aware that preservation requests for the email address: **demsoft@gmail.com** were sent on December 11, 2011, and January 5, 2015. I am aware that preservation requests for the email address: **cosma2k@gmail.com** were sent on January 9, 2012, and January 5, 2015. I am also aware that, in general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time. Based on my training and experience, I have determined that individuals involved in spamming and other online criminal activities tend to retain emails for extended periods of time. For example, I am aware that, during the investigation of Oleg Nikolaenko, he retained emails in his Gmail account for more than five years.

BACKGROUND CONCERNING EMAIL

32. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts

listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

34. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. I further know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

35. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

36. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

38. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a

time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with email addresses: cosma2k@gmail.com, and demsoft@gmail.com that are stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a requests made under 18 U.S.C. § 2703(f) on December 11, 2011, and January 5, 2015, **(demsoft@gmail.com)** and on January 9, 2012, and January 5, 2015, **(cosma2k@gmail.com)**, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

Information to be seized by the government

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1030 and 1037, those violations involving Dmitry Nijegorodtsev and occurring between January 2007, and September 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications related to sending spam email messages.

b. Communications related to malware and/or computer viruses.

c. Communications related to computer botnets.

d. Communications related to Genbucks, Sancash, and Affking affiliate programs.

e. Communications related to the iContact data breach;

f. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

g. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

h. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

i. The identity of the person(s) who communicated with these email addresses about matters relating to the above-described offense conduct, including records that help reveal their whereabouts.